CLAIMS

1. A method comprising:

selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and

decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet.

2. A method in accordance with claim 1, wherein the applying comprises performing a bit per bit streaming encryption process.

3. A method in accordance with claim 2, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

4. A method in accordance with claim 2, wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet.

5. A method in accordance with claim 2, further comprising:

receiving the data packet, the data packet comprising at least a portion of the received session count.

6. A method in accordance with claim 5, wherein the data packet further comprises at least a portion of a received message digest value.

7. A method in accordance with claim 5, wherein the selecting comprises:

selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value.

8. A method in accordance with claim 7, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

9. A method in accordance with claim 8, further comprising:

discarding the data packet if the difference is not less than the threshold value.

10. A method in accordance with claim 9, further comprising:

re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference in not less than the threshold value.

11. A method in accordance with claim 6, further comprising:

discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value.

12. A method in accordance with claim 11, further comprising:

re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value.

13. A method in accordance with claim 12, further comprising:

extracting the at least a portion of the received message digest value from the data packet;

generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key;

truncating the locally generated message digest value to form a truncated message digest; and

comparing the truncated message digest to the at least a portion of the received message digest value.

14. A method of generating an encrypted data packet, the method comprising:

selecting a fixed length segment of a continuous encryption key stream;

applying a portion of the fixed length segment to data to form an encrypted payload;

generating a session count based in accordance with the fixed length segment; and

combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet.

15. A method in accordance with claim 14, wherein the applying comprises performing a bit per bit streaming encryption process.

16. A method in accordance with claim 15, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

17. A method in accordance with claim 15, wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet.

18. A method in accordance with claim 14, further comprising:

generating a message digest value; and

combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet.

19. A method in accordance with claim 18, wherein the generating comprises:

generating the message digest value based on the encrypted payload, the session count and a message digest key.

20. A method in accordance with claim 18, further comprising:

forming the at least a portion of the message digest value by truncating the message digest value.

21. A method in accordance with claim 14, further comprising transmitting the encrypted data packet to a receiver through a communication channel.

22. A method in accordance with claim 14, further comprising:

receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value;

selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and

decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet.

23. A method in accordance with claim 22, wherein the applying comprises performing a bit per bit streaming decryption process.

24. A method in accordance with claim 22, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

25. A method in accordance with claim 22, wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet.

26. A method in accordance with claim 25, wherein the selecting the fixed length segment of the continuous decryption key stream comprises:

selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value.

27. A method in accordance with claim 26, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the received encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

28. A method in accordance with claim 27, further comprising:

discarding the received encrypted data packet if the difference is not less than the threshold value.

29. A method in accordance with claim 28, further comprising:

re-synchronizing the decryption key to the encryption key by setting the decryption key and the encryption key to a start vector if the difference in not less than the threshold value.

30. A method in accordance with claim 26, further comprising:

discarding the received encrypted data packet if the received truncated message digest value does not match a truncated locally generated message digest value.

31. A method in accordance with claim 30, further comprising:

re-synchronizing the decryption key stream to an encryption key stream by setting the decryption key stream and the encryption key stream to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value.

32. A method in accordance with claim 31, further comprising:

extracting the received truncated message digest value from the received encrypted data packet;

generating a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key;

truncating the locally generated message digest value to form the locally generated truncated message digest value; and

comparing the locally generated truncated message digest value to the received truncated message digest value.

33. A receiver comprising:

a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold; and

a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold.

34. A receiver in accordance with claim 33, wherein the decryption engine is further configured to perform a bit per bit streaming encryption process.

35. A receiver in accordance with claim 34, wherein the decryption engine is further configured to perform an exclusive OR operation with the portion of the fixed length segment and the data packet.

36. A receiver in accordance with claim 34, wherein the decryption engine is further configured to perform an RC4 operation with the portion of the fixed length segment and the data packet.

37. A receiver in accordance with claim 33, wherein the received encrypted data packet comprises at least a portion of the session count.

38. A receiver in accordance with claim 37, further comprising:

a session count extractor configured to extract the at least a portion of the received session count from the received encrypted data packet; and

a session count expander configured to expand the at least a portion of the received session count to the received session count.

39. A receiver in accordance with claim 38, wherein the received encrypted data packet further comprises at least a portion of a received message digest value.

40. A receiver in accordance with claim 39, further comprising:

a message digest extractor configured to extract the at least a portion of the received message digest value from the received encrypted data packet;

a message digest generator configured to generate a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key;

a truncator configured to truncate the locally generated message digest value to form a truncated message digest; and

a message digest evaluator configured to compare the truncated message digest value to the at least a portion of the received message digest value, wherein the receiver is configured to discard the received encrypted data packet if the truncated message digest value does not match the at least a portion of the received message digest value.

41. A transmitter configured to generate an encrypted data packet, the transmitter comprising:

an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload;

a session count generator configured to generate a packet number in accordance with the fixed length segment, the encrypted data packet comprising the encrypted payload and at least a portion of the session count.

42. A transmitter in accordance with claim 41, wherein the encryption engine is configured to perform a bit per bit streaming encryption process.

43. A transmitter in accordance with claim 42, wherein the encryption engine is further configured to perform an exclusive OR operation with the portion of the fixed length segment and the data packet.

44. A transmitter in accordance with claim 42, wherein the encryption engine is further configured to perform an RC4 operation with the portion of the fixed length segment and the data packet.

45. A transmitter in accordance with claim 42, further comprising:

a message digest generator configured to generate a message digest value, the encrypted data packet comprising at least a portion of the message digest value.

46. A transmitter in accordance with claim 45, wherein the message digest generator is further configured to generate the message digest value based on the encrypted payload, the session count and a message digest key.

47. A transmitter in accordance with claim 46, further comprising:

a truncator configured to truncate the message digest value to form the at least a portion of the message digest value.

48. A system comprising:

a transmitter configured to generate an encrypted data packet, the transmitter comprising:

an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload;

a session count generator configured to generate a session count in accordance with the fixed length segment; the encrypted data packet comprising the encrypted payload and at least a portion of the session count; and

a receiver configured to receive the encrypted data packet, the receiver comprising:

a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold; and

a decryption engine configured to decrypt the encrypted payload by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold.

49. A method comprising:

receiving a data packet through a communication channel; the data packet comprising at least a portion of a session count;

selecting a fixed length segment of a continuous decryption key stream based on the session count; and

applying a portion of the fixed length segment by performing a bit per bit streaming encryption to decrypt a payload of the data packet.

50. A method in accordance with claim 49, wherein the selecting comprises:

selecting a current fixed length segment if a difference between the received session count and the locally generated session count is less than a threshold value.

51. A method in accordance with claim 50, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

52. A method in accordance with claim 51, further comprising:

discarding the data packet if the difference is not less than the threshold value.

53. A method of generating an encrypted data packet, the method comprising:

selecting a fixed length segment of a continuous encryption key stream;

applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload;

generating a session count in accordance with the fixed length segment; and

combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet.